The ProtonMail Guide to IT Security

for Small Businesses

Protect your network

The ProtonMail IT security team

Protect your network

READ THIS CHAPTER to identify the IT security best practices your IT security leader should be in charge of, including:

- Network security basics
- Creating a secure internal network
- Maintaining user security
- Log auditing
- Advanced network security
- Data backups
- IT security admin best practices list

Network security sounds complicated, but at its heart, it is straightforward. Similar to how you lock up your office, you must lock up your network to keep your data safe. You must be able to prevent and react to the unauthorized access to and abuse of your network. This requires having technological solutions, documentation, processes, and an IT security leader or admin to control the flow of information over your company's system. While this IT security leader should be able to handle the more technical aspects of network management, their job is impossible unless your staff regularly implements IT security best practices (See Chapter 2).

Your network encompasses all your devices, including computers, laptops, workstations, servers, tablets, or smartphones and all of their connections, either to each other over a local area network or to the Internet. This could be as simple as two laptops sharing documents over the cloud or as complex as companies that have their own internal networks running off private servers.

This chapter gives a basic outline of the responsibilities of your IT security leader and what they should do to maintain your network security.

IT security leader basics

Just as every company handles different data, each company faces unique threats. Precautions that would make sense for one company may not be necessary for another. For example, most small businesses that are not focused on information technology do not need to concern themselves with an internal network or a firewall or a SIEM. Instead, they should focus on taking simple steps that can significantly reduce their business's vulnerability.

Train employees on IT security

The most critical step is training your staff and cultivating a culture of IT security awareness. (See Chapter 2)

Remind employees about phishing attacks and describe new threats

IT security threats are constantly evolving. Hackers are continually exploiting new bugs and creating new types of social engineering attacks. Keep your employees and colleagues up to date by sending out a brief email update on the latest and most popular threats. These updates will help them recognize any hacking or phishing attempts they might encounter.

Conduct a brief assessment of employee adherence to the Employee IT security best practices list

Without regular tests and reminders, even the most conscientious employees can forget about IT security best practices. Conduct a simple test or hold a brief meeting to make sure your employees and colleagues are adhering to IT security best practices. These evaluations or meetings are also an excellent time to address any questions about IT security your employees or colleagues might have.

Create a database of approved devices

But before the training even begins, your IT security leader should create a comprehensive database of all the devices that connect to your company's network or have access to its data. Each one of these devices is a potential weak point. Your IT security leader should ensure that all network-connected devices, including smartphones, are using a firewall and full disk encryption.

Establish permission levels for employees and devices

Once you know which devices will be connecting to your network, your IT security leader should create different levels of access to your company's data, depending on what that employee does. This includes physical access to sensitive network devices and hard-copy files. No employee should have access to portions of data that are not essential to their day-to-day tasks. Only pre-approved employees should be able to download or install new programs on their device.

Use privacy-focused services

Look into replacing software or applications that your business uses to handle sensitive data with privacy-focused services. These types of programs or apps generally use end-to-end encryption (E2EE) to keep information inaccessible except to its owner (and, depending on the service, its intended recipient). Chapter 4 has a comprehensive list of a range of privacy-focused services your business can use.

Creating a secure internal network

As your business grows, you will need to adjust your IT security precautions. Eventually, you will need to start putting in place technological tools, like your own business WiFi network, internal servers, and a firewall. This will also require an IT security leader with more technical expertise as well.

You should follow the steps below as your business grows. Using a secure WLAN can be done by companies of any size, but implementing a firewall, segmenting your network, or using a corporate VPN only apply to businesses that run their own internal network.

WLAN Security

Nearly every business needs Internet access to handle day-to-day tasks. To be secure, you need to have your own, dedicated WiFi router. All WiFi routers sold since 2006 use the WiFi Protected Access 2 protocol, which is currently the most secure. If you are concerned, check your wireless card or device for a "Wi-Fi CERTIFIED" label to see if it uses WPA2.

The next step is to make sure you use the Enterprise mode of WPA2—also known as 802.11i. This is more complex to set up than a standard WiFi network, but it offers several essential security advantages, the most important of which are the elimination of shared passwords and WiFi snooping.

Set up a network firewall

A properly configured firewall is your internal network's first line of defense. It filters the data of your network or device and only allows permitted traffic through. If your corporate network is connected to the Internet, a perimeter firewall will prevent bad actors from accessing your network by blocking traffic that doesn't meet a predetermined set of criteria.

Segment your network

Segmenting your network is the best way to prevent a full system failure from occurring if a malicious actor or malware make it past your firewall. If your network is segmented, even if one server is compromised, the malware can be contained, and the rest of your IT infrastructure can continue functioning. You should base the decision of how to segment your network on the sensitivity of the data being handled and where the traffic is initiated. A server that is accessible from the Internet should not be located on the same network as a server containing sensitive data.

There are three ways you should think about segmenting your network: using Network address translation (NAT), maintaining separate WiFi networks for employees and guests, and creating virtual local area networks (VLAN).

Your employees' devices should not have their own, public IP addresses. NAT allows several computers on the same network to share one public IP address at the same time. If your company employs a dynamic NAT, you add another layer of protection between your internal network and the Internet, as the NAT will only allow connections that devices from your system initiate.

Your business WiFi network should not be shared with guests. Even with WPA2 Enterprise, allowing untrusted devices onto your WiFi poses the risk of introducing malware into your network. Restricting visitors to a separate WiFi network segment will also prevent them from accessing internal services, such as network files and printers. Finally, it gives you a greater measure of control over your guests' WiFi without affecting your employees' WiFi.

Finally, make sure your employees' devices and your corporate servers are connected to different VLAN. A VLAN is an example of software-defined network segmentation. It partitions and isolates parts of a single physical network so that network applications can be kept apart.

Use a corporate VPN

A firewall will protect and segment your network, but today, more and more employees are working remotely. You need to find a way for them to securely access your corporate data so that they can do their jobs. This is different from a VPN service that will encrypt your Internet connection. While it will use the same type of protocols (OpenVPN or IKEv2), a corporate VPN creates an encrypted connection over the Internet to your company's corporate server, letting your employees safely download and transmit files without any fear of malicious actors intercepting or manipulating your data.

Advanced IT security leader best practices

Once your company has established its own internal network, your IT security leader's responsibilities will dramatically change, as will the expertise necessary for the job. In addition to keeping your staff trained and up to date, they will have to work much more extensively with the technological tools you have put in place to secure your system.

Maintaining user security

Reassess role-based access management and separation of duties

Companies are not static. New employees come, old employees are promoted, projects end and new ones are reassigned. The turnover of the business cycle means that the type and amount of data that an employee should have access to is continuously shifting. By keeping employees' access limited to only the data they need to perform their day-to-day tasks, you reduce the chance of a catastrophic breach if one account is compromised. Your IT security leader should regularly assess which employees have access to which data and confirm with their supervisor that that level of permission is appropriate. Role-based access control will need to be implemented to define which user is allowed to access which data.

Disable old or obsolete accounts

Old, unused, and inactive accounts are a security threat. Your admin must disable them in a regular and timely manner.

Always check to make sure there is not a reason these accounts have been inactive (like that employee is gone on vacation or parental leave). Also, check to see if any employees have recently been fired or quit, and have them added to the list. Once the list is prepared, and your IT security leader has double-checked it, they should go through and disable user accounts one at a time.

Log auditing

Review security information and system logs (with a SIEM, if applicable)

Every device on your company's network should produce comprehensive event logs that you can search, filter, and review. These logs will help your IT security leader catch any emerging issues or security threats early on.

These reports should all go into a centralized location. By having the reports and records all in place, you can search for abnormal behavior and make sure they are not modified by accident or deleted or altered maliciously.

A SIEM (security information and event management) system aggregates data from

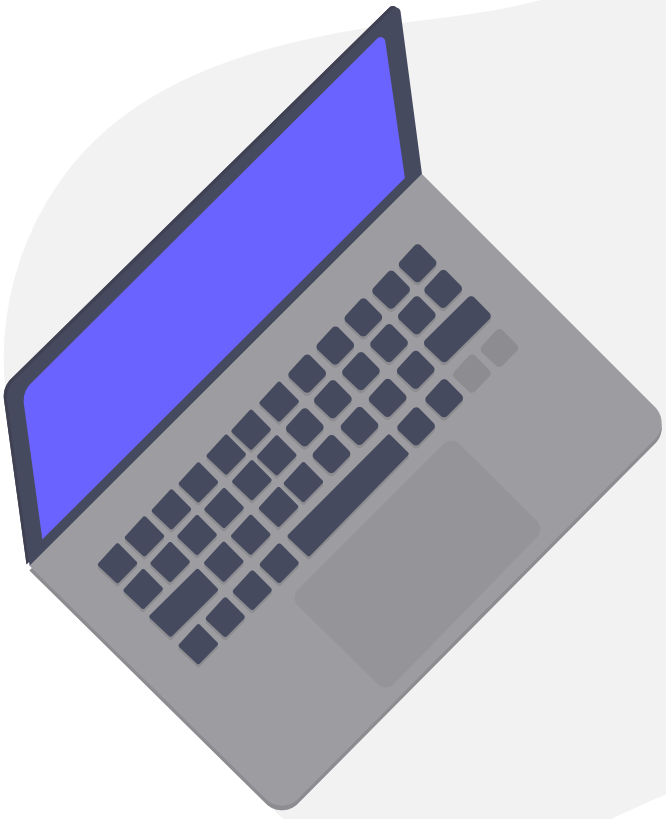
your network and uses rules-based or statistical correlation engines to determine what normal activity on your network looks like, identify any deviations, and take appropriate action. A SIEM system also allows you to view in one place all the logs and records your network generates, making it much easier to spot suspicious patterns. While this is a more advanced tool that should be employed on larger networks, if your company's network does have a SIEM system, check it regularly.

Whether your IT security leader uses a SIEM or manually checks your system's logs, they should do it on a regular basis to make sure nothing unusual has been detected and to make sure the logs are being recorded as expected. If an attack or a failure happens and they do not have any records to go over, it will be difficult to find and solve the problem.

Review user activity and remote access logs

The easiest way to start spotting suspicious activity is by looking at who is logging in and from where. If someone is logging in remotely after you just saw them in the office, or if someone who has been fired has just logged in, there may be foul play involved. Your IT security leader should regularly review these logs, flag all suspicious logins, and follow up by contacting the account owner to find out what they were doing. If the employee is unaware of the login or has reason to think their account may have been compromised, your IT security leader should check to see if any sensitive data was accessed and take measures to ensure the account's security (like changing its password or temporarily suspending the account).

- Flag any suspicious logins.
- Record who was involved, what happened, and when it happened.
- Check to see if any sensitive data was accessed.
- Take action to secure data/account.



Advanced network security

Check computer lifecycle and update as necessary

Your list of all network-connected devices must expand to include all your business's servers and workstations. This inventory should be updated anytime new systems or hardware are integrated into your network.

Check software lifecycle and update as necessary

In addition to a list of all your devices and hardware, you should maintain and append a comprehensive list of all the software you are using on them, along with their most recent update. Software updates are often released to fix known bugs. By using an old version of a program, you are introducing a vulnerability into your system. This inventory should be updated anytime software or applications are integrated into your network.

Your IT security leader should also regularly check online to see if there are new versions of any of the programs you are using. If one has been updated, then download the update (or email fellow employees to download the update). Then open up your software inventory and add the details of this update, new program, or application.

Check and install latest security patches (with SCAP, if applicable)

Failing to carry out regular security patches is one of the most common points of failure in any computer network, and often holes appear as a result of bad processes in systems' maintenance.

SCAP, or the Security Content Automation Protocol, is an automated system that will scan your system searching for vulnerable versions of software. Using SCAP lets your company benefit from the entire SCAP community of IT security experts. They define the different configurations and use cases that SCAP should look out for, making SCAP a comprehensive vulnerability scanning tool.

Test your firewall security

Your IT security leader should regularly check your firewall security to make sure that your company's servers cannot be accessed from the outside through an unknown port.

They should run a scan to make sure the only ports on your network that are open are the ones they have whitelisted. Perform an external to internal port scan with Nmap.

- Check which ports are supposed to be opened.
- Perform a remote scan with Nmap and compare the result.

Evaluate firewall configuration

If the firewall security test did not perform as expected, then your IT security leader should evaluate the firewall configuration.

To make sure the firewall is configured properly, your admin should look at the different settings your firewall offers and adjust them to resolve the issue you found. To do this, they will need to also validate the authorized flow of traffic into your system as well as between internal zones (if applicable).

They should go through the sub-checklist below to troubleshoot the basic settings that might have caused the firewall security test to fail.

- Check anti-spoofing filters.
- Check user permit rules.
- Check system administrator alert settings.
- Check system traffic log analysis.

Test and run antivirus software

Antivirus is a preventative measure. It works to detect, quarantine, and remove any known malware that makes it on to your system. Ideally, your network will not be flooded with malware, and so it may be hard to know if your antivirus is doing its job sometimes. But given the essential role antivirus software plays in your overall network security, and especially for workstations or servers dealing with files, it is crucial your IT security leader tests your antivirus software regularly.

They can test the resilience of your antivirus software by downloading an EICAR file designed to simulate a virus or malware infection. EICAR files are completely safe and used by IT security experts to see if antivirus programs are working as they should.

Follow the process in the sub-checklist below.

- Download the EICAR file.
- Run an isolated scan for the EICAR file.

Your system's antivirus software should detect the EICAR file, alert you, and quarantine it. If it does not, you should strongly consider getting new antivirus software.

Following the EICAR test, perform a full system scan:

- Launch your antivirus software control panel.
- Perform a full system scan.
- Isolate and quarantine any threats detected.

Data backups

Making backups of your business's data is not necessarily part of network security. It is more like your insurance policy in case your network security fails. If ransomware compromises your company's devices or if there is a system failure, these backups will help your company get back on its feet.

Check and back up system data

Your IT security leader needs to make regular backups of all your most vital data. Remember, it is better to be over-inclusive than for a system crash to halt your business because you did not save the correct folder. Ideally, the backup process will be automated.

Even if the backup process is automated, your admin needs to regularly verify that all the processes are running smoothly and that the data are actually being saved.

- Ensure servers are fully backed up.
- Ensure workstations are fully backed up.

Making sure the backups are working and accessible is just as important as checking to make sure the data are being backed up in the first place. Using a random sample of files from the most recent backup, your IT security leader should try opening them on a workstation machine to see if the data are accessible. You should test at least three backup files to get a more reliable result.

- Take three backup images made in the last week.
- Load them all onto the same configuration as their parent system.
- Check they are all working as expected.

Evaluate backup process

If the backup files your IT security leader tested were inaccessible or corrupted, they must now locate the problem in your automated backup system. Finding the problem can require extensive testing at each stage of the automatic backup process, including re-saving and re-testing system-wide backup files or changing to a new automated backup process.

- Perform backup process troubleshooting.
- Test three more random backup samples.
- Evaluate your current backup process.
- Consider changing to a new backup process.

ProtonMail

Acknowledged as a global leader in online security and privacy, ProtonMail automatically applies end-to-end, zero-access encryption to its messages. This makes it the email of choice for journalists, dissidents, activists, and anyone concerned about protecting their online communications.

Headquartered in Geneva, Switzerland, with offices around the world, ProtonMail provides private and secure email services to thousands of businesses of all sizes. To learn more about using ProtonMail for your business, click here.